Attorney's Docket No.: 16491-009002

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: CONTROLLING ACCESS TO A MEDICAL MONITORING SYSTEM

APPLICANT: DOUG C. EVELAND, WILLIAM R. MARABLE AND BOBBY E. ROGERS

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. EV 399312217 US

December 5, 2003

Date of Deposit

CONTROLLING ACCESS TO A MEDICAL MONITORING SYSTEM

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority under 35 U.S.C. 120 to U.S. application serial no. 09/841,154, to be issued on December 16, 2003, as U.S. Patent 6,664,893, the disclosure of which is incorporated by reference.

BACKGROUND

[0002] The following description relates to controlling access to a medical monitoring device and/or a service associated with the device, for example, to help ensure that access to the monitoring device and service are authorized prior to commencing usage.

[0003] Advances in sensor technology, electronics, and communications have made it possible for physiological characteristics of patients to be monitored even when the patients are ambulatory and not in continuous, direct contact with a hospital monitoring system. For example, U.S. Patent 5,959,529 describes a monitoring system in which the patient carries a remote monitoring unit with associated physiological sensors. The remote monitoring unit conducts a continuous monitoring of one or more physiological characteristics of the patient according to the medical problem of the patient, such as the heartbeat and its waveform.

[0004] One potential issue associated with the use of such medical monitoring devices is establishing whether the patient's health-care-benefit payer has authorized the use of the monitoring device and service. In the absence of a proper authorization, the patient may use the medical monitoring device and incur significant charges, for example, in the form of rental value of the medical monitoring device, telephone charges, charges at the central monitoring system, and charges by medical personnel, and the providers of those goods and services may not get paid. Bad debts – an increasing concern in the medical field generally – tend to be an even

greater concern in the case of a portable medical monitoring device and its service where the physical control of the device is in the hands of a third party, such as a prescribing doctor, who does not own the medical monitoring device and is not responsible for improper charges.

SUMMARY

[0005] The present inventors recognized a need for an approach to controlling access to medical monitoring devices and their associated services to help ensure that only a properly authorized patient can use the service. Controlling access to a medical monitoring system may be accomplished by a system and/or technique that includes one or more of the following features.

[0006] To control access to a medical monitoring system, a computer-based method may involve receiving information indicating that a remote monitoring device (e.g., a patient-portable device configured to monitor one or more physiological aspects of a patient) seeks access (e.g., through one or more communications links including either or both of a wired communication link and a wireless communication link) to a monitoring service hosted by a central unit, and determining whether the remote monitoring device is authorized to access the monitoring service. This determination is based at least in part on authorization data received from a third-party source. Based on a result of the determination, an activation signal is selectively issued to the remote monitoring device.

[0007] The determination of whether the remote monitoring device is authorized to access the monitoring service may be performed cooperatively between the remote device and the central unit. Further, the determination of whether the remote monitoring device is authorized to access the monitoring service may include one or both of (i) performing a format

check on access data entered into the remote monitoring device and (ii) comparing the entered access data against the third-party authorization data.

[0008] The access control method may further include maintaining, at the central unit, a local database of third-party authorization data to be used in the determination of whether the remote monitoring device is authorized to access the monitoring service. The local authorization database may be updated, for example, periodically or based on a predetermined event or a combination of both.

[0009] Selectively issuing the activation signal to the remote monitoring device based on a result of the determination may include issuing the activation signal if the remote monitoring device is determined to be authorized to access the medical monitoring service and refraining from issuing an activation signal if the remote monitoring device is determined to be unauthorized to access the medical monitoring service.

[0010] In another aspect, a medical monitoring system centered at a central node includes one or more communications links configured to facilitate communications with remote monitoring devices (e.g., a patient-portable device configured to monitor one or more physiological aspects of a patient) and one or more third-party authorization sources. The medical monitoring system also includes at least one programmable processor configured to perform various operations. These operations may include hosting a medical monitoring service (e.g., implemented at least in part by one or more software processes), receiving information indicating that a remote monitoring device seeks access to the medical monitoring service hosted by a central unit, determining, based at least in part on authorization data received from a third-party authorization source, whether the remote monitoring device is authorized to access the monitoring service, and based on a result of the determination, selectively issuing an activation signal to the remote monitoring device.

[0011] The programmable processor may further be configured to maintain at the central node a local database of third-party authorization data to be used in the determination of whether the remote monitoring device is authorized to access the monitoring service. The local authorization database may be updated based on data received from the one or more third-party authorization sources. Updating may occur periodically or based on a predetermined event or a combination of both.

[0012] The programmable processor may further be configured to determine whether the remote monitoring device is authorized to access the monitoring service by one or both of (i) performing a format check on access data entered into the remote monitoring device and (ii) comparing the entered access data against the third-party authorization data.

[0013] The programmable processor may be configured to issue the activation signal to the remote monitoring device if the remote monitoring device is determined to be authorized to access the medical monitoring service and to refrain from issuing an activation signal if the remote monitoring device is determined to be unauthorized to access the medical monitoring service.

[0014] In another aspect, a portable medical monitoring device includes a transceiver for communicating with a central node, a user interface for communicating with a user of the device, and a programmable processor configured to perform various operations. These operations may include receiving user input specifying user-specific information, transmitting the received user input to the central node for third-party authorization based at least in part on the user-specific information, and selectively providing the user with access to a monitoring service hosted at the central node based on a result of the third-party authorization.

[0015] The programmable processor further may be configured to perform a format check on the received user input to determine whether the user input meets one or more

predetermined criteria. If the user input is determined not to meet one or more of the predetermined criteria, the programmable processor may refrain from transmitting the received user input to the central station and/or may deny access to the monitoring service. In addition, the programmable processor may be configured to provide access to the monitoring service if the device receives an activation signal from the central node and to deny access to the monitoring service if the device fails to receive an activation signal from the central node.

[0016] Among other potential advantages, the systems and techniques described here may facilitate controlling access to medical monitoring devices and associated services. The approach may help to ensure that service is initiated and continued only for persons who are properly authorized to have the service. For example, the present approach may activate the medical monitoring device and its corresponding service only for a person who provides proper identification data and is financially and otherwise properly authorized for the service. As a result, the chances of a wrong person being monitored may tend to be reduced. The activation process, which may involve the input of proper identification data, may be quick and largely transparent to the person seeking the service.

[0017] The systems and techniques described here may help to ensure that medical monitoring device services are provided only to properly identified and authorized persons. They may also help to ensure that all persons and agencies responsible for the medical monitoring device and the services are coordinated in their approval of rendering service to the particular patient and in effect have approved the provision of service and the type of service to be provided. Potential legal and financial liability may thereby be reduced. Other features and advantages will be apparent from the following detailed description, the accompanying drawings, and the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Figure 1 is a flow diagram of a method of controlling access to a medical monitoring device and/or an associated service.

[0019] Figure 2 is a,schematic illustration of a system for implementing the method of Figure 1.

DETAILED DESCRIPTION

[0020] Figure 1 depicts a flow diagram of a method of controlling access to a medical monitoring device and/or service. A medical monitoring device and its associated system are provided (20). The medical monitoring device and medical monitoring system may be of any operable type, such as that disclosed in US Patent 5,959,529 (hereafter, "the '529 patent"), whose disclosure is incorporated in its entirety, and/or modified as discussed herein.

[0021] Figure 2 depicts details, in block diagram form, of a medical monitoring system 50 that includes a medical monitoring device system 52, which in turn comprises a medical monitoring device 54 and a base station 56. The medical monitoring device 54 may be a portable or remote monitoring unit of the type generally described in the '529 patent. The base station 56 has communication access to a central unit 58 through a communication link such as a wireless cellular telephone transceiver link 60 and/or a telephone land-line 62. Alternatively, or in addition, communication links can be established by other available means, among others, such as wired or wireless networks that implement communications protocols and standards such IP (Internet protocol), WiFi (IEEE 802.11x), WiMax (IEEE 802.16x), and GPRS (General Packet Radio Service). The central unit 58, typically maintained at a central node or location, may in practice be composed of multiple computer systems distributed across, or even outside of, the central node.

[0022] In the implementation shown in Fig. 2, the base station 56 has a base station cradle 64 that is configured to receive the medical monitoring device 54 therein and establishes communication between the medical monitoring device 54 and an input/output device 65 that typically includes a microprocessor, communications controller, and communications hardware and/or software to establish the links 60 and/or 62. The input/output device 65 has a keypad 66 for inputting information and a display 68 to view the input information and other information to be displayed, as well as information transmitted to the input/output device 65.

[0023] The central unit 58 has communications access to a variety of databases 71 and to third-party sources 72, typically by telephone land-line, network or other connection 70. The databases 71 may include prior patient records, general records, and the like. The third-party sources 72 may include, for example, financial sources 74, medical sources 76, and other sources 78. A financial source might be, for example, an insurance company, the social-security administration, or a credit-granting company. A medical source might be, for example, a specialist physician whose authorization is required before commencing the monitoring of the patient. Other third-party sources might be, for example, the company that maintains the medical monitoring device 54 and which is consulted to be certain that the specific medical monitoring device to be activated is approved for service.

[0024] The base station 56, when not prescribed or otherwise assigned and distributed to a patient to be monitored, ordinarily is in the custody the office of the agency that is providing the medical monitoring device 54 to a patient for the purpose of monitoring physiological parameters of the patient. Such an agency could be, for example, the patient's physician or a hospital. When the agency undertakes to provide the medical monitoring device 54 to the patient, for example, to take home, the medical monitoring device 54 is docked with the base station 56, and the procedures described in relation to subsequent portions of Figure 1 are followed.

[0025] Returning to Figure 1, a set of identification data elements (22) are input into the medical monitoring device system 52 through the keypad 66 of the input/output device 65 of the base station 56 in the system 50 of Figure 2. The identification data elements may include, for example, a patient name, a patient address, a patient social security number, a patient sex, and an identification of the third-party financial source. The identifier of the medical monitoring device 54, such as its serial number, may be manually input in step 22, but more normally the identifier is automatically made available by the medical monitoring device 54 to the base station 56.

[0026] The base station 56 may perform a preliminary evaluation of the set of identification data elements, for example, such as to determine by using a software utility program whether the identification data elements meet a set of one or more format requirements. Such basic format requirements may be specified for each of the identification data elements. For example, a format requirement may specify that a patient name is to include only alphanumeric characters. If as typed into the keyboard the patient name includes other characters (e. g., a percent sign %), software running in the base station can recognize the error and provide an input diagnostic message through the display 68 to prompt the input of correct information. In another example, a format requirement may specify that a user's social security number must contain 10 numerical digits and may not contain letters or other characters.

[0027] After what appears from the preliminary format evaluation to be a set of correct identification data elements is input to the medical monitoring device system 52, the medical monitoring device system 52 establishes (24) a communication link to the central unit 58. The communication link is preferably through the land-line 62, but may be though the cellular telephone transmission link 60 or another wireless or wired link if the land-line is not available.

[0028] The medical monitoring device system 52 and the central unit 58 cooperatively determine whether the medical monitoring device 54 may be activated for rendering medical

monitoring device service (26). The final decision is typically made by the central unit 58, although the medical monitoring device system 52 may aid in data processing or may be called upon for additional input, for example, such as when the patient name is found not to match with the social security number in other records.

[0029] The activation determination process 26 may include various sub-processes including evaluating the set of identification data elements as to whether they meet a set of basic structural requirements (28) and obtaining third-party authorization (30) from one or more of the third-party sources 72. The sub-processes of evaluating 28 and obtaining 30 are preferably performed automatically. "Automatically" as used means herein that the steps are performed without human action or intervention, except where a discrepancy occurs. The present system is organized to perform the evaluating and obtaining steps entirely by computer procedures, to minimize costs and take advantage of data collections at a variety of locations. Alternatively, the present approach may be performed in whole or in part using manual (i.e., human-performed) sub-processes 28 and 30. In addition, the sub-process 30 of obtaining third-party authorization can be performed either before or during the activation determination process 26. For example, the sub-process 30 may involve updating a locally stored (e.g., at a central unit hosting the medical monitoring service) copy of a third party's database of authorization information, and then performing the sub-process 30 by accessing the local copy of the database instead of accessing the third party's system, which typically would be maintained at a remote location. Updating of the local third-party authorization database may occur based on one or both of the following criteria: (i) periodically (e.g., once a day) or (ii) based on an occurrence of a predetermined event (e.g., the third-party system determines that a certain amount of new authorization data is available and has not yet been copied to the central unit's local database and/or the central unit determines that its local database does not contain needed information).

[0030] The set of basic structural requirements to be imposed may include the format requirements evaluated by the base station 56, or may include different or additional structural requirements. For example, the central unit 58 may check the database 71 to attempt to match the input patient name with a social security number that is already in the database 71 from prior medical contacts. If the patient name and the social security number that were input in sub-process 22 do not match, then further inquiry may be made back to the medical monitoring device system 52. The failure to match the name and the social security number may arise from a simple inputting error, which can be corrected with revised input, or it may arise from a fraudulent attempt to obtain medical monitoring services that is detected by the procedures of sub-process 28.

[0031] As noted above, obtaining third-party authorization in sub-process 30 may include contacting appropriate third-party sources 72, e.g., either on a dynamic, as-needed basis, and/or ahead of time by periodically replicating a third party's remote database to create a local copy. The financial source 74 may be contacted to determine whether it authorizes the charges associated with the patient monitoring services. This authorization is particularly important for the business interests of the provider of the services, for example, to avoid unpaid billings. Unpaid billings for medical services represents a major loss for many medical service companies. The medical source 76 may be contacted to determine whether it authorizes the patient monitoring. For example, if the prospective patient is being treated by more than one physician, it may be important to obtain authorization from each physician who is treating the patient before medical monitoring services are commenced. In this case, "authorization" signals formal recognition by the authorizing party that monitoring information will be available. Other sources 78 may also be contacted to determine whether they authorize the patient monitoring. For example, it may be desirable to ensure that the company responsible for maintaining the specific

medical monitoring device 54 to be activated authorizes its use. If a prior user had reported a problem and the specific medical monitoring device 54 had been taken out of service for repair, but was mistakenly to be re-activated without being repaired, the company responsible for the maintenance could prevent its activation at this stage.

[0032] Thus, the procedures in sub-process 26 act as a "sign off" by a number of checks and third-parties to minimize the possibility that a medical monitoring device will be wrongly issued to a patient and activated. If the sign-offs are not completed, the medical monitoring device is not activated until the reason for the non-completion may be investigated. It is expected that in the great majority of cases, the activation determination process 26 will be completed without incident and so rapidly that the checking will be transparent to the patient and the issuer of the medical monitoring device.

[0033] Based on results of the activation determination process, the activation decision is made (32). The final decision is typically made at the central unit 58, although all or part of the final decision could be made at the base station and/or distributed or made by a system at another location. Typically, the decision is made at the central unit 58 because it has the access to the required information during the activation determination process 26, and because the central unit 58 tends to be more immune to tampering than the base station 56.

[0034] In the event that the identification data elements meet the set of basic structural requirements and third-party authorization is obtained, the central unit 58 issues an activation signal (34) to the medical monitoring device system 52 over the communication link 60 or 62. The medical monitoring device 54 is activated and enters service (36).

[0035] The "activation signal" may be of any operable type. It may be a software "on" switch that enables the processing of data within a microprocessor in the medical monitoring device 54 or a hardware "on" switch that turns on particular hardware functions such as the

communications links built into the medical monitoring device 54. The activation signal may be complex, and may include identification of the patient and the specific medical monitoring device 54 that is associated with that patient. This activation signal may then be transmitted with each subsequent communication between the medical monitoring device 54 and the central unit 58 for identification purposes. In the event that the proper activation signal is not transmitted with each communication, it may be ignored. The activation may be revoked (38) at a later time if the authorization is withdrawn or for other reasons. Upon revocation 38, the signals transmitted by the medical monitoring device 54 are not acted upon, and the patient and/or the issuing authority are notified and requested to return the medical monitoring device 54. As an alternative to revocation 38, the activation signal of step 34 may include a maximum time limit for which activation is authorized, so that a further authorization is required to extend the period of authorized use.

[0036] Other embodiments are within the scope of the following claims.